

AN ULTRAMETRIC SPACE OF EISENSTEIN POLYNOMIALS AND RAMIFICATION THEORY

MANABU YOSHIDA

ABSTRACT. We give a criterion whether given Eisenstein polynomials over a local field K define the same extension over K in terms of a certain non-Archimedean metric on the set of polynomials. The criterion and its proof depend on ramification theory.

1. INTRODUCTION

Let K be a complete discrete valuation field, k its residue field (which may be imperfect) of characteristic $p > 0$, v_K its valuation normalized by $v_K(K^\times) = \mathbb{Z}$, \mathcal{O}_K its valuation ring, Ω a fixed algebraic closure of K and \bar{K} the separable closure in Ω . The valuation v_K can be extended to Ω uniquely and the extension is also denoted by v_K . Let L/K be a finite Galois extension with ramification index e and inertia degree 1. Denote by \mathcal{O}_L the integral closure of \mathcal{O}_K in L . Take a uniformizer π_L of \mathcal{O}_L and its minimal polynomial f over K , which is an Eisenstein polynomial over K . Let E_K^e be the set of all Eisenstein polynomials over K of degree e . For two polynomials $g = \sum a_i X^i, h = \sum b_i X^i \in E_K^e$, we put

$$v_K(g, h) := \min_{0 \leq i \leq e-1} \{v_K(a_i - b_i) + \frac{i}{e}\}.$$

Then the function $v_K(\cdot, \cdot)$ defines a non-Archimedean metric on E_K^e (cf. Lem. 3.1). For any $g \in E_K^e$, we put $M_g = K(\pi_g)$, where π_g is a root of g . For any real number $m \geq 0$, we consider the following property:

(T_m^e) *For any $g \in E_K^e$, if $v_K(f, g) \geq m$, then there exists a K -isomorphism $L \cong M_g$.*

This property does not depend on the choice of π_L (cf. Prop. 6.1). Let $u_{L/K}$ be the largest upper numbering ramification break of L/K in the sense of [Fo] (cf. Sect. 2). Then we can prove the following (Prop. 4.1):

Proposition 1.1. *The property (T_m^e) is true for $m > u_{L/K}$, and is not true for $m \leq u_{L/K} - e^{-1}$.*

This proposition is a consequence of results of Fontaine on a certain property (P_m) (cf. Appendix). Since both $v_K(f, g)$ and $u_{L/K}$ are in $e^{-1}\mathbb{Z}$, the truth of (T_m^e) is constant for $u_{L/K} - e^{-1} < m \leq u_{L/K}$. Therefore, we want to know the truth of (T_m^e) for $m = u_{L/K}$. The property (T_m^e) behaves mysteriously at the break

2010 *Mathematics Subject Classification.* Primary: 11S15, Secondly: 11S05.

Key words and phrases. Eisenstein polynomials, Ramification theory.

The author is supported by the Japan Society for the Promotion of Scientist Fellowships for Young Scientists.

$m = u_{L/K}$. It depends on the ramification of L/K and the residue field k . Our main theorem in this paper is the following (Cor. 5.3):

Theorem A. *If L/K is tamely ramified, then (T_m^e) is true for $m = u_{L/K}$ if and only if the residue field k has no cyclic extension of degree e . If L/K is wildly ramified, then (T_m^e) is true for $m = u_{L/K}$ if and only if the residue field k has no cyclic extension of degree p .*

We reduce the proof of this theorem to the abelian case by showing that (T_m^e) is equivalent to a certain property (P_m^e) , which has such a reduction property (Prop. 6.3). To prove the abelian case, we show that, by using the properties of the ultrametric space E_K^e , the truth of the property (T_m^e) for $m = u_{L/K}$ is equivalent to the surjectivity of the norm map $N_{m-1} : U_L^{\psi(m-1)}/U_L^{\psi(m-1)+1} \rightarrow U_K^{m-1}/U_K^m$ between the graded quotients of the higher unit groups of L and K , where ψ is the Hasse-Herbrand function of L/K (Prop. 6.5). Finally, we calculate its cokernel by using the well-known exact sequence (Prop. 6.8)

$$0 \rightarrow G_{\psi(m-1)}/G_{\psi(m-1)+1} \rightarrow U_L^{\psi(m-1)}/U_L^{\psi(m-1)+1} \xrightarrow{N_{m-1}} U_K^{m-1}/U_K^m,$$

where G_i is the i th lower numbering ramification group in the sense of [Se] (cf. Rem. 2.2). The vanishing of $\text{Coker}(N_{m-1})$ is equivalent to the conditions in Theorem A.

Our results are useful for computations to construct explicit extensions over K which satisfy given conditions. For example, such computations are required in [SY], [YY1] and [YY2]. Indeed, the proof of Proposition 5.1, (1) in [SY] is based on our results. In [YY1] and [YY2], our approaches are used to identify totally ramified extensions over \mathbb{Q}_p .

Plan of this paper. In Section 2, we give a review of the classical ramification theory. In Section 3, we recall a notion of ultrametric space on polynomials. In Section 4, we define the property (T_m^e) , which is the main object in this paper. In Section 5, we state our main theorem and its consequences. In Section 6, we prove the main theorem. In the Appendix, we consider similar properties (P'_m) and (P_m) . To remove confusion, we clarify the relation between the four properties which appear in this paper:

$$(P_m) \iff (P'_m) \implies (P_m^e) \iff (T_m^e),$$

where the last equivalence requires the condition $m > 1$.

Notations. We fix an algebraic closure Ω of K and denote by \bar{K} the separable closure of K in Ω . We denote by \mathcal{O}_K , \mathfrak{m}_K , π_K and v_K , respectively, the valuation ring of K , its maximal ideal, a uniformizer of K and the valuation on K normalized by $v_K(K^\times) = \mathbb{Z}$. We assume throughout that all algebraic extensions of K under discussion are contained in Ω . The valuation v_K of K extends to Ω uniquely and the extension is also denote by v_K . If M is an algebraic extension of K , then we denote by \mathcal{O}_M the integral closure of \mathcal{O}_K in M , and by \mathfrak{m}_M the maximal ideal of \mathcal{O}_M . For any integer $n \geq 1$, we put $U_K^n = 1 + \mathfrak{m}_K^n$ and $U_L^n = 1 + \mathfrak{m}_L^n$. Put $U_K^0 = \mathcal{O}_K^\times$ and $U_L^0 = \mathcal{O}_L^\times$ by convention.

Conventions. Throughout this paper, we assume that L/K is unferociously ramified¹ extension. We do not consider the trivial case $L = K$.

Acknowledgments. The author thanks Takashi Suzuki for communicating Proposition 6.8 to him. He also thanks Kazuya Kato for suggesting an improvement of the proof of Lemma 6.2. Finally, he thanks Yuichiro Taguchi for pointing out Remark 2.5.

2. RAMIFICATION THEORY

In this section, we recall the classical ramification theory for Galois extensions of K . Our notations are based on [Fo], Section 1. Let L be a finite Galois extension of K with Galois group G . There exists an element $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (the existence of such an element is proved in [Se], Chap. III, Sect. 6, Prop. 12). The order function $\mathbf{i}_{L/K}$ is defined on G by

$$\mathbf{i}_{L/K}(\sigma) = \inf_{a \in \mathcal{O}_L} v_K(\sigma(a) - a) = v_K(\sigma\alpha - \alpha)$$

for any $\sigma \in G$. Then the i th lower numbering ramification group $G_{(i)}$ of G are defined for a real number $i \geq 0$ by

$$G_{(i)} = \{\sigma \in G \mid \mathbf{i}_{L/K}(\sigma) \geq i\}.$$

The transition function $\tilde{\varphi}_{L/K} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ of L/K is defined by

$$\tilde{\varphi}_{L/K}(i) = \int_0^i \#G_{(t)} dt$$

for any real number $i \geq 0$, where $\#G_{(t)}$ is the cardinality of $G_{(t)}$. This is a piecewise-linear, monotone increasing function, mapping the interval $[0, +\infty)$ onto itself. Its inverse function is denoted by $\tilde{\psi}_{L/K}$. The following lemma is a fundamental property of these functions:

Lemma 2.1 ([Fo], Prop. 1.4). *Let L be a finite Galois extension of K . Let f be the minimal polynomial of α over K and β an element of Ω . Put $i = \sup_{\sigma \in G} v_K(\sigma(\alpha) - \beta)$ and $u = v_K(f(\beta))$. Then we have*

$$u = \tilde{\varphi}_{L/K}(i), \quad \tilde{\psi}_{L/K}(u) = i.$$

We define the order function $\mathbf{u}_{L/K}$ on G by

$$\mathbf{u}_{L/K}(\sigma) = \tilde{\varphi}_{L/K}(\mathbf{i}_{L/K}(\sigma))$$

for any $\sigma \in G$. Then the u th upper numbering ramification group $G^{(u)}$ of G are defined for a real number $u \geq 0$ by

$$G^{(u)} = \{\sigma \in G \mid \mathbf{u}_{L/K}(\sigma) \geq u\}.$$

Remark 2.2. Denote by G_i , G^u , $\varphi_{L/K}$ and $\psi_{L/K}$, respectively, the i th lower numbering ramification group, the u th upper numbering ramification group, the transition function and its inverse function in the sense of [Se], Chapter IV. The relation between our notations and those of [Se] is the following: For any real number $i, u \geq -1$, we have

$$G_i = G_{((i+1)/e)}, \quad G^u = G^{(u+1)}$$

¹ We mean by an *unferociously* ramified extension an algebraic extension whose residue field extension is separable.

and

$$\varphi_{L/K}(i) = \tilde{\varphi}_{L/K}((i+1)/e) - 1, \quad \psi_{L/K}(u) = e\tilde{\psi}_{L/K}(u+1) - 1,$$

where e is the ramification index of L/K .

Denote the largest lower (resp. upper) numbering ramification break by

$$i_{L/K} = \inf\{i \in \mathbb{R} \mid G_{(i)} = 1\}, \quad u_{L/K} = \inf\{u \in \mathbb{R} \mid G^{(u)} = 1\}.$$

The graded quotients of $(G^{(u)})_{u \geq 1}$ are abelian and killed by p ([Se], Chap. IV, Sect. 2, Cor. 3). In particular, $G^{(u)}$ is abelian and killed by p for $u = u_{L/K}$ if L/K is wildly ramified.

We assume that L/K is totally ramified. If there is no confusion, we write $\psi = \psi_{L/K}$ for simplicity.

Proposition 2.3 ([Se], Chap. V, Prop. 8). *For any integer $n \geq 0$, $N(U_L^{\psi(n)}) \subset U_K^n$ and $N(U_L^{\psi(n)+1}) \subset U_K^{n+1}$, where $N := N_{L/K}$ is the norm map.*

This proposition allows us, by passage to the quotient, to define the homomorphisms

$$N_n : U_L^{\psi(n)} / U_L^{\psi(n)+1} \rightarrow U_K^n / U_K^{n+1} \quad (n \geq 0).$$

The homomorphism N_n is a non-constant polynomial map ([Se], Chap. V, Sect. 6, Prop. 9).

Proposition 2.4 ([Se], Chap. V, Sect. 6, Prop. 9). *For any integer $n \geq 0$, the following sequence is exact:*

$$0 \rightarrow G_{\psi(n)} / G_{\psi(n)+1} \xrightarrow{\theta_n} U_L^{\psi(n)} / U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n / U_K^{n+1},$$

where θ_n is defined by $\sigma \mapsto \sigma(\pi_L) / \pi_L$.

Remark 2.5. The polynomial N_n is separable since θ_n is injective. Hence if the residue field k is separably closed, then we have

$$0 \rightarrow G_{\psi(n)} / G_{\psi(n)+1} \xrightarrow{\theta_n} U_L^{\psi(n)} / U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n / U_K^{n+1} \rightarrow 0.$$

3. AN ULTRAMETRIC SPACE OF MONIC IRREDUCIBLE POLYNOMIALS

In this section, we define a non-Archimedean metric on the set, denoted by P_K , of all monic irreducible polynomials over K . For $f, g \in P_K$, we denote by $\text{Res}(f, g)$ the resultant of f and g . Then $v_K(\text{Res}(\cdot, \cdot))$ defines a non-Archimedean metric on P_K (see [Kr] or [PR], Sect. 4 for the proofs). It is well-known that

$$v_K(\text{Res}(f, g)) = \sum_{i,j} v_K(\alpha_i - \beta_j) = \deg(f)v_K(f(\beta)) = \deg(g)v_K(g(\alpha)),$$

where α_i (resp. β_j) runs through the all roots of f (resp. g) and α (resp. β) is a root of f (resp. g). The third and forth presentations are independent of the choice of roots by the irreducibility of polynomials. Denote by E_K^e the set of all Eisenstein polynomials over K of degree e . For $f, g \in E_K^e$, we put

$$v_K(f, g) = e^{-1}v_K(\text{Res}(f, g)) = v_K(f(\pi_g)),$$

where the last equality follows from the above equality. Then the function $v_K(\cdot, \cdot)$ also defines a non-Archimedean metric on E_K^e . There is a useful formula to calculate the metric on E_K^e :

Lemma 3.1 ([Kr]). *Let $f, g \in E_K^e$. Write $f(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$ and $g(X) = X^e + b_{e-1}X^{e-1} + \cdots + b_0$. Then we have*

$$v_K(f, g) = \min_{0 \leq i \leq e-1} \{v_K(a_i - b_i) + \frac{i}{e}\}.$$

4. THE PROPERTY (T_m^e)

In this section, we define the property (T_m^e) and determine the truth for any real number $m \geq 0$ except a neighborhood of the break $u_{L/K}$. The proofs in this section essentially depend on [Fo], Proposition 1.5. Let L/K be a finite Galois totally ramified extension of degree e . Take a uniformizer π_L of L . Let $f \in E_K^e$ be the minimal polynomial of π_L over K . For any $g \in E_K^e$, we put $M_g = K(\pi_g)$, where π_g is a root of g . For any real number $m \geq 0$, we consider the following property:

(T_m^e) For any $g \in E_K^e$, if $v_K(f, g) \geq m$, then there is a K -isomorphism $L \cong M_g$.

Let $u_{L/K}$ be the upper numbering ramification break of L/K . Then we have the following:

Proposition 4.1. (i) *If $m > u_{L/K}$, then (T_m^e) is true.*

(ii) *If $m \leq u_{L/K} - e^{-1}$, then (T_m^e) is not true.*

Proof. (i) By assumption, we have $v_K(f, g) = v_K(f(\pi_g)) \geq m > u_{L/K}$. According to Lemma 2.1, we have

$$\sup_{\sigma \in G} v_K(\pi_g - \sigma(\pi_L)) = \tilde{\psi}_{L/K}(v_K(f(\pi_g))) > \tilde{\psi}_{L/K}(u_{L/K}) = i_{L/K}.$$

Hence there exists $\sigma_0 \in G$ such that

$$v_K(\pi_g - \sigma_0(\pi_L)) > i_{L/K} = \sup_{\sigma \neq 1} v_K(\sigma(\pi_L) - \pi_L) = \sup_{\sigma \neq 1} v_K(\sigma(\sigma_0(\pi_L)) - \sigma_0(\pi_L)).$$

By Krasner's lemma, we have $L \cong K(\sigma_0(\pi_L)) \subset K(\pi_g) = M_g$.

(ii) This follows from Lemma 4.2 below immediately. \square

Lemma 4.2. *Let $g \in E_K^e$. If $v_K(f, g) = u_{L/K} - e^{-1}$, then we have $L \not\cong M_g$.*

Proof. By assumption, we have $v_K(f(\pi_L)) = v_K(f, g) = u_{L/K} - e^{-1}$. By Lemma 2.1, we have

$$\sup_{\sigma \in G} v_K(\pi_g - \sigma(\pi_L)) = \tilde{\psi}_{L/K}(u_{L/K} - e^{-1}) = i_{L/K} - \frac{1}{ed},$$

where $d := \sharp G^{(u_{L/K})}$. By multiplying e with the above equation, we have

$$v_L(\pi_g - \sigma_0 \pi_L) = ei_{L/K} - \frac{1}{d},$$

for some $\sigma_0 \in G$. If we suppose $L = M_g$, then LHS is an integer. However, RHS is never an integer. This is a contradiction. Hence we have $L \neq M_g$. \square

5. MAIN THEOREM

In this section, we state our main theorem and its consequences. Let L/K be a finite totally ramified Galois extension of degree e .

Theorem 5.1. *The property (T_m^e) for $m = u_{L/K}$ is equivalent to the condition $\text{Hom}_{\text{cont}}(G_k, G_{(i_{L/K})}) = 1$.*

Corollary 5.2. *Assume k is a quasi-finite field. Then (T_m^e) is not true for $m = u_{L/K}$.*

Proof. By assumption, we have

$$\text{Hom}_{\text{cont}}(G_k, G_{(i_{L/K})}) = \text{Hom}_{\text{cont}}(\hat{\mathbb{Z}}, G_{(i_{L/K})}) \cong G_{(i_{L/K})} \neq 1.$$

We obtain the desired result by Theorem 5.1. \square

Theorem A is a consequence of the following:

Corollary 5.3. *If L/K is tamely ramified, then (T_m^e) for $m = u_{L/K}$ is equivalent to the condition $k^\times / (k^\times)^e = 1$. If L/K wildly ramified, then (T_m^e) for $m = u_{L/K}$ is equivalent to the condition $k/\wp(k) = 0$, where $\wp(X) := X^p - X$.*

Proof. Assume L/K is tamely ramified. Then the group $G = G_{(i_{L/K})}$ is isomorphic to a finite cyclic group μ_e of order e . Note that k contains the e th roots of unity. Hence we have $\text{Hom}_{\text{cont}}(G_k, \mu_e) \cong k^\times / (k^\times)^e$ by Kummer theory. It follows the desired result by Theorem 5.1. Assume L/K is wildly ramified. Then we have $G_{(i_{L/K})} \cong \oplus \mathbb{Z}/p\mathbb{Z}$. Therefore, we obtain $\text{Hom}_{\text{cont}}(G_k, G_{(i_{L/K})}) \cong \oplus k/\wp(k)$ by Artin-Schreier theory. By Theorem 5.1, the proof completes. \square

6. PROOF OF THE MAIN THEOREM

6.1. Reduction to the abelian case. In this subsection, we reduce the proof of Theorem 5.1 to the case where L/K has only one ramification break so that L/K is abelian. To complete this, we consider the property (P_m^e) below. Let L/K be a finite Galois totally ramified extension of degree e .

(P_m^e) *For any finite totally ramified extension M/K of degree e , if there exists an \mathcal{O}_K -algebra homomorphism $\mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$, then there exists a K -isomorphism $L \cong M$.*

Proposition 6.1. *The property (T_m^e) is equivalent to (P_m^e) for any real number $m > 1$.*

Proof. Let L/K be a finite Galois totally ramified extension of degree e . Take a uniformizer π_L of L and $f \in E_K^e$ its minimal polynomial over K . Assume that (T_m^e) is true for f and $m > 1$. Then we show that (P_m^e) is also true for L/K and m . Suppose there exists an \mathcal{O}_K -algebra homomorphism $\eta : \mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$ for a totally ramified extension M of K of degree e . By Lemma 6.2 below, we have $v_K(\beta) = 1/e$, where β is a lift of $\eta(\pi_L)$ in \mathcal{O}_M . Hence β is a uniformizer of M . Take the minimal polynomial $g \in E_K^e$ of β over K . By the well-definedness of η , we have $v_K(f, g) = v_K(f(\beta)) \geq m$. Since the property (T_m^e) is true for f and m , we have $L = M_g \cong M$.

Conversely, we assume that (P_m^e) is true for L/K and $m > 1$. Then we show that (T_m^e) is also true for f and m . Suppose $v_K(f, g) \geq m$ for an element $g \in E_K^e$. Note that $v_K(f(\pi_g)) = v_K(f, g) \geq m$, where π_g is a root of g . Then the map

$\mathcal{O}_L \rightarrow \mathcal{O}_{M_g}/\mathfrak{a}_{M_g/K}^m$ defined by $\pi_L \mapsto \pi_g$ is an \mathcal{O}_K -algebra homomorphism. Since (P_m^e) is true for L/K and m , we have $L \cong M_g$. \square

Lemma 6.2. *Let L/K be a finite totally ramified extension of degree e , π_L a uniformizer of L and $m > 1$ a real number. Assume there exists an \mathcal{O}_K -algebra homomorphism $\eta : \mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$ for an algebraic extension M of K . Then we have $v_K(\beta) = 1/e$, where β is any lift of $\eta(\pi_L)$.*

Proof. Assume there exists an \mathcal{O}_K -algebra homomorphism $\eta : \mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$. Put $u = \pi_L^e/\pi_K$. Then u is a unit, so that $\eta(u)$ is also. Since $\beta^e \equiv \eta(u)\pi_K$ in $\mathcal{O}_M/\mathfrak{a}_{M/K}^m$ and $m > 1$, we have $v_K(\beta^e) = v_K(\pi_K) = 1$. Hence $v_K(\beta) = 1/e$. \square

Proposition 6.3. *Let L be a finite Galois totally ramified extension of K of degree e and K' the fixed field of L by $H := G^{(u_{L/K})}$. Take a uniformizer π_L of L . Let f (resp. f') be the minimal polynomial of π_L over K (resp. K'). Then the property (T_m^e) is true for f and $m = u_{L/K}$ if and only if $(T_m^{e'})$ is true for f' and $m = u_{L/K'}$, where e' is the ramification index of L/K' .*

Proof. If L/K is tamely ramified, then we have $K = K'$. Hence there is nothing to prove. Thus we may assume L/K is wildly ramified, so that $m = u_{L/K} > 1$. By definition, L/K' is also wildly ramified, so that $m = u_{L/K'} > 1$. By Proposition 6.1, (T_m^e) for f and $m = u_{L/K}$ is equivalent to (P_m^e) for L/K and $m = u_{L/K}$. Similarly, $(T_m^{e'})$ for f' and $m = u_{L/K'}$ is equivalent to $(P_m^{e'})$ for L/K' and $m = u_{L/K'}$. Thus it is enough to prove that (P_m^e) for L/K and $m = u_{L/K}$ is equivalent to $(P_m^{e'})$ for L/K' and $m = u_{L/K'}$. This is a direct consequence of the following lemma:

Lemma 6.4 ([SY], Lem. 2.2). *Let L and K' be as in Proposition 6.3. Let M be an algebraic extension of K . The following conditions are equivalent:*

- (i) *There exists an \mathcal{O}_K -algebra homomorphism $\mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^{u_{L/K}}$.*
- (ii) *The field K' is contained in M , and there exists an $\mathcal{O}_{K'}$ -algebra homomorphism $\mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K'}^{u_{L/K'}}$.*

\square

6.2. The proof of the abelian case. In this subsection, we complete the proof of Theorem 5.1. It suffices to show the abelian case by Proposition 6.3. Then the break $u_{L/K}$ is an integer by the Hasse-Arf theorem ([Se], Chap. V, Sect. 7, Thm. 1). Therefore, it suffices to prove the integer break case:

Proposition 6.5. *Assume $u_{L/K}$ is an integer. Then Theorem 5.1 is true.*

Proof. Put $m = u_{L/K}$. Let L/K be a finite Galois totally ramified extension of degree e such that $u_{L/K}$ is an integer. Take a uniformizer π_L of L and its minimal polynomial f over K . Let $g \in E_K^e$. Put $M_g = K(\pi_g)$, where π_g is a root of g . We write $f = X^e + a_{e-1} + \cdots + a_0$ and $g = X^e + b_{e-1} + \cdots + b_0$. We want to show that if $v_K(f, g) = m$, then the equality $L = M_g$ is equivalent to the condition $\text{Hom}_{\text{cont}}(G_k, G_{(i_{L/K})}) = 1$.

First, we prove that it suffices to consider g of the following form by replacing f with suitable one:

$$g = g_u := X^e + a_{e-1}X^{e-1} + \cdots + a_1X + ua_0,$$

where u is an element of $U_K^{m-1} \setminus U_K^m$. By Lemma 3.1 and the assumption that $u_{L/K}$ is an integer, we have

$$v_K(f(\pi_g)) = \min_{0 \leq i \leq e-1} \{v_K(a_i - b_i) + \frac{i}{e}\} = v_K(a_0 - b_0) = m.$$

Thus we have $b_0 = ua_0$ for some $u \in U_K^{m-1} \setminus U_K^m$. Let $f_0 := X^e + b_{e-1}X^{e-1} + \dots + b_1X + a_0$. Note that $v_K(f, f_0) = \min_{1 \leq i \leq e-1} \{v_K(a_i - b_i) + i/e\} > m$. According to Proposition 4.1, the extension defined by f_0 coincides with L . By replacing f with f_0 , we reduce the problem to the desired situation.

Second, we show that $L = M_u$ for any $u \in U_K^{m-1} \setminus U_K^m$ if and only if the map N_{m-1} is surjective, where M_u/K is the extension defined by g_u and N_{m-1} is the norm map defined in Section 2. Assume $L = M_u$ for any $u \in U_K^{m-1} \setminus U_K^m$. By Lemma 2.1, we have $v_K(\sigma_0(\pi_L) - \pi_{M_u}) = i_{L/K}$ for some $\sigma_0 \in G$. Take $u' := \pi_{M_u}/\sigma_0(\pi_L) \in L = M_u$. Note that $v_L(1 - u') = ei_{L/K} - 1$ by the equality $v_K(\sigma_0(\pi_L) - u'\sigma_0(\pi_L)) = i_{L/K}$ and $\psi(m-1) = ei_{L/K} - 1$ by Remark 2.2. Thus we have $u' \in U_L^{\psi(m-1)} \setminus U_L^{\psi(m-1)+1}$. Moreover, we have $ua_0 = N(\pi_{M_u}) = N(u'\sigma(\pi_L)) = N(u')N(\sigma(\pi_L)) = N(u')a_0$, so that we have $N(u') = u$. Conversely, we assume that the map N_{m-1} is surjective. Then there exists an element u' of $U_L^{\psi(m-1)} \setminus U_L^{\psi(m-1)+1}$ such that $N(u') = u$. Note that $\pi'_L := u'\pi_L$ is a uniformizer of L and $v_K(\pi'_L - \pi_L) = i_{L/K}$. Let f' be the minimal polynomial of π'_L over K . By Lemma 6.7 below, we have $v_K(\pi'_L - \pi_L) = \sup_{\sigma \in G} v_K(\pi'_L - \sigma(\pi_L))$. According to Lemma 2.1, we have

$$\begin{aligned} v_K(f, f') &= v_K(f(\pi'_L)) \\ &= \tilde{\varphi}_{L/K}(\sup_{\sigma \in G} v_K(\pi'_L - \sigma(\pi_L))) = \tilde{\varphi}_{L/K}(v_K(\pi'_L - \pi_L)) \\ &= \tilde{\varphi}_{L/K}(i_{L/K}) = u_{L/K} = m. \end{aligned}$$

By the ultrametric inequality, we have

$$v_K(g_u, f') \geq \min\{v_K(f, g_u), v_K(f, f')\} = m.$$

The constant term of f' is the same as the one of g_u . Then we have $v_K(g_u, f') \neq m$ by Lemma 3.1 and that m is an integer. Thus we have $v_K(g_u, f') > m$. According to Lemma 2.1, we have $L = M_u$. Therefore, we reduce the truth of (T_m^e) for $m = u_{L/K}$ to the surjectivity of the map N_{m-1} . Thus it is enough to prove $\text{Coker}(N_{m-1}) \cong \text{Hom}_{\text{cont}}(G_k, G_{(i_{L/K})})$. It follows from Lemma 6.8 below immediately as $n = m - 1$. \square

Remark 6.6. In the proof of Theorem 6.5, we do not require the assumption that L/K is abelian. We need only the assumption that $u_{L/K}$ is an integer.

Lemma 6.7. *We have*

$$v_K(\pi'_L - \sigma(\pi_L)) \begin{cases} < i_{L/K} & \sigma \in G \setminus G_{(i_{L/K})} \\ = i_{L/K} & \sigma \in G_{(i_{L/K})}. \end{cases}$$

Therefore, we have $v_K(\pi'_L - \pi_L) = i_{L/K} = \sup_{\sigma \in G} v_K(\pi'_L - \sigma(\pi_L))$.

Proof. Suppose $\sigma \notin G_{(i_{L/K})}$. Then we have $v_K(\pi_L - \sigma(\pi_L)) < i_{L/K}$. Hence we have

$$\begin{aligned} v_K(\pi'_L - \sigma(\pi_L)) &= v_K(\pi'_L - \pi_L + \pi_L - \sigma(\pi_L)) \\ &= \min\{v_K(\pi'_L - \pi_L), v_K(\pi_L - \sigma(\pi_L))\} \\ &= \min\{i_{L/K}, v_K(\pi_L - \sigma(\pi_L))\} < i_{L/K}. \end{aligned}$$

Next, we consider the case $\sigma \in G_{(i_{L/K})}$. Then we have $v_K(\pi_L - \sigma(\pi_L)) = i_{L/K}$ so that $\pi_L/\sigma(\pi_L) \in U_L^{ei_{L/K}-1}$. Note that

$$v_K(\pi'_L - \sigma(\pi_L)) = v_K(u' \frac{\pi_L}{\sigma(\pi_L)} - 1) + \frac{1}{e}.$$

To prove that RHS is equal to $i_{L/K}$, we show $u' \cdot \pi_L/\sigma(\pi_L) \in U_L^{ei_{L/K}-1} \setminus U_L^{ei_{L/K}}$. This is equivalent to $u' \cdot \pi_L/\sigma(\pi_L) \not\equiv 1$ in $U_L^{ei_{L/K}-1}/U_L^{ei_{L/K}}$. To prove this, it suffices to show $N(u' \cdot \pi_L/\sigma(\pi_L)) \not\equiv 1$ in U_K^{m-1}/U_K^m by considering the norm map $N_{m-1} : U_L^{\psi(m-1)}/U_L^{\psi(m-1)+1} \rightarrow U_K^{m-1}/U_K^m$ with $\psi(m-1) = ei_{L/K} - 1$. Since $N(u') \not\equiv 1 \pmod{U_K^m}$ and $N(\pi_L/\sigma(\pi_L)) = 1$, we have $N(u' \cdot \pi_L/\sigma(\pi_L)) = N(u')N(\pi_L/\sigma(\pi_L)) = N(u') \not\equiv 1 \pmod{U_K^m}$. \square

Lemma 6.8. *Let L be a totally ramified Galois extension of K and n be an integer ≥ 0 . Then we have*

$$\text{Coker}(N_n) \cong \text{Hom}_{\text{cont}}(G_k, G_{\psi(n)}/G_{\psi(n)+1}).$$

Proof. Let K_0 (resp. L_0) be the completion of the maximal unramified extension of K (resp. L). Apply Proposition 2.4 to L_0/K_0 . Then the sequence

$$0 \rightarrow G_{\psi(n)}/G_{\psi(n)+1} \rightarrow U_{L_0}^{\psi(n)}/U_{L_0}^{\psi(n)+1} \rightarrow U_{K_0}^n/U_{K_0}^{n+1} \rightarrow 0$$

is exact. The Galois group G_k acts on L_0 and K_0 continuously. Define the action of G_k on G_n/G_{n+1} by the trivial action. Since L/K is totally ramified, the action of G on L_0 is compatible with G_k -action. Thus the above sequence is exact as continuous G_k -modules. Writing out the corresponding exact cohomology sequence, and taking into account that $H_{\text{cont}}^1(G_k, \bar{k}) = 0$, we obtain

$$k \rightarrow k \rightarrow H_{\text{cont}}^1(G_k, G_{\psi(n)}/G_{\psi(n)+1}) \rightarrow 0.$$

Consequently, we have $\text{Coker}(N_n) \cong H_{\text{cont}}^1(G_k, G_{\psi(n)}/G_{\psi(n)+1})$. Since G_k acts on $G_{\psi(n)}/G_{\psi(n)+1}$ trivially, this is equal to $\text{Hom}_{\text{cont}}(G_k, G_{\psi(n)}/G_{\psi(n)+1})$. Hence the result follows. \square

Remark 6.9. This lemma is a generalization of [Se], Chapter XV, Section 2, Proposition 3.

7. APPENDIX

Throughout this appendix, we assume that k is perfect. We consider a property (P'_m) , which is similar to (T_m^e) . We completely determine the truth of (P'_m) by showing that (P'_m) is equivalent to (P_m) . Let L be a finite Galois extension of K . Take an element α of \mathcal{O}_L such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Let f be the minimal polynomial of α over K and P_K the set of all monic irreducible polynomials over K . For any $g \in P_K$, we put $M_g = K(\beta)$, where β is a root of g . Consider the following property for any real number $m \geq 0$:

(P'_m) For any $g \in P_K$, if $v_K(\text{Res}(f, g)) \geq \deg(g)m$, then there exists a K -embedding $L \hookrightarrow M_g$.

If f and g are contained in E_K^e , then $v_K(\text{Res}(f, g)) \geq \deg(g)m$ is equivalent to $v_K(f, g) \geq m$. Hence the property (P'_m) is stronger than (T_m^e) .

For a finite Galois extension L/K and real numbers $m \geq 0$, we consider the following property:

(P_m) For any algebraic extension M/K , if there exists an \mathcal{O}_K -algebra homomorphism $\mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$, then there exists a K -embedding $L \hookrightarrow M$.

Fontaine proved the following:

Proposition 7.1 ([Fo], Prop. 1.5). *Let L be a finite Galois extension of K and e the ramification index of L/K . Then there are following relations:*

- (i) *If $m > u_{L/K}$, then (P_m) is true.*
- (ii) *If $m \leq u_{L/K} - e^{-1}$, then (P_m) is not true.*

The author proved the following:

Proposition 7.2 ([Yo], Prop. 3.4). *Let L be a finite Galois extension of K . If $m < u_{L/K}$, then (P_m) is not true.*

As a similar result of our main theorem, the truth of (P_m) at the ramification break depends on the ramification of L/K and the residue field k :

Proposition 7.3 ([SY], Thm. 1.1). *Let L be a finite Galois wildly ramified extension of K . Then the property (P_m) is true for $m = u_{L/K}$ if and only if k has no Galois extension whose degree is divisible by p .*

Remark 7.4. If L/K is at most tamely ramified, then (P_m) is not true for $m = u_{L/K}$. This is shown in the proof of Proposition 3.3, [Yo].

In fact, we have the following:

Proposition 7.5. *For any real number $m \geq 0$, (P'_m) is equivalent to (P_m).*

Proof. Let L be a finite Galois extension of K . Choose an element $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Let f be the minimal polynomial of α over K . Assume that (P'_m) is true for f and m . Then we show that (P_m) is also true for L/K and m . Suppose there exists an \mathcal{O}_K -algebra homomorphism $\eta : \mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$ for an algebraic extension M of K . Let β be a lift of $\eta(\alpha)$ in \mathcal{O}_M . Then we have $v_K(f(\beta)) \geq m$. Let g be the minimal polynomial of β over K . Then we have $v_K(\text{Res}(f, g)) = \deg(g)v_K(f(\beta)) \geq \deg(g)m$. By the property (P'_m), there exists a K -embedding $L \hookrightarrow K(\beta) \subset M$. Conversely, assume that (P_m) is true for L/K and m . Then we show that (P'_m) is also true for L/K and m . Suppose $v_K(\text{Res}(f, g)) \geq \deg(g)m$ for an arbitrary polynomial $g \in P_K$. Then we have $v_K(f(\beta)) \geq m$, where β is a root of g . Put $M = K(\beta)$. The map $\mathcal{O}_L \rightarrow \mathcal{O}_M/\mathfrak{a}_{M/K}^m$ defined by $\alpha \mapsto \beta$ is an \mathcal{O}_K -algebra homomorphism. By the property (P_m), there exists a K -embedding $L \hookrightarrow M$. \square

Therefore, we have the following two consequences from Propositions 7.1, 7.2 and 7.3:

Corollary 7.6. *Let L be a finite Galois extension of K . Then the property (P'_m) is true for $m > u_{L/K}$, and is not true for $m < u_{L/K}$.*

Corollary 7.7. *Let L be a finite Galois wildly ramified extension of K . Then the property (P'_m) is true for $m = u_{L/K}$ if and only if k has no Galois extension whose degree is divisible by p .*

REFERENCES

- [Fo] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur \mathbb{Z}* , Invent. Math. **81** (1985) no. 3, 515–538
- [Kr] M. Krasner, *Nombre des extensions d'une degré donné d'un corps \mathfrak{P} -adique*, Les Tendances Géométriques en Algèbre et Théorie des Nombres, Ed. CNRS, Paris, 1966
- [PR] S. Pauli and X.-F. Roblot, *On the computations of all extensions of p -adic field of a given degree*, Math. Comp. **70** (2001) no. 236, 1641–1659
- [Se] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer-Verlag (1979)
- [SY] T. Suzuki and M. Yoshida, *Fontaine's property (P_m) at the maximal ramification break*, arXiv.org:1012.2935.
- [YY1] S. Yokoyama and M. Yoshida, *An identification for Eisenstein polynomials of degree p over a p -adic field*, arXiv.org:1105.5520.
- [YY2] S. Yokoyama and M. Yoshida, *Generating program for all abelian extensions of a p -adic field*, preprint
- [Yo] M. Yoshida, *Ramification of local fields and Fontaine's property (P_m)*, J. Math. Sci. Univ. Tokyo **17** (2010) no. 3, 247–265

GRADUATE SCHOOL OF MATHEMATICS, KYUSHU UNIVERSITY, FUKUOKA 819-0395, JAPAN
E-mail address: m-yoshida@math.kyushu-u.ac.jp